



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/862,801

05/22/2001

Vitaly Neyman

655/63958

1154

5073

7590

11/02/2005

BAKER BOTTS L.L.P.  
2001 ROSS AVENUE  
SUITE 600  
DALLAS, TX 75201-2980

EXAMINER

ZAND, KAMBIZ

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 11/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Advisory Action  
Before the Filing of an Appeal Brief**

Application No.

09/862,801

Applicant(s)

NEYMAN ET AL.

Examiner

Kambiz Zand

Art Unit

2132

**--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

THE REPLY FILED 28 September 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.  
b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**NOTICE OF APPEAL**

2. ☐ The Notice of Appeal was filed on \_\_\_\_\_. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

**AMENDMENTS**

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because  
(a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);  
(b) ☐ They raise the issue of new matter (see NOTE below);  
(c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or  
(d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: \_\_\_\_\_. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): \_\_\_\_\_.

6. ☐ Newly proposed or amended claim(s) \_\_\_\_\_ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: \_\_\_\_\_.

Claim(s) objected to: \_\_\_\_\_.

Claim(s) rejected: 1-32.

Claim(s) withdrawn from consideration: \_\_\_\_\_.

**AFFIDAVIT OR OTHER EVIDENCE**

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

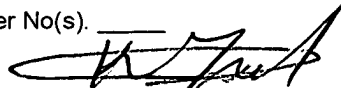
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

**REQUEST FOR RECONSIDERATION/OTHER**

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:  
See Continuation Sheet.

12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). \_\_\_\_\_

13. ☐ Other: \_\_\_\_\_.



Kambiz Zand  
Examiner  
Art Unit: 2132

Continuation of 11. does NOT place the application in condition for allowance because: 1- As per applicant's arguments that "the required evidence of a motivation to combine and /or modify prior art references is lacking" on last paragraph of page 20 of the applicant's response dated 09/28/2005, examiner refer applicant's to the following remarks:

a) Applicant's invention related to malicious code detection method using heuristic logic as described on the Title of the invention and the field of the disclosure on page 1 of the specification.

b) Joyce invention also relates analyzing packet streams using heuristic logic by monitoring the packets and detecting malicious codes and analyzing the results as described in abstract and col.3, lines 29-67 where malicious codes such as computer viruses such as Torjan signatures.

Therefore the Applicant's invention and the Joyce invention are within the same technological environment and fields of art.

c) Joyce disclose monitoring the packets and analyzing them and selecting the appropriate action based on the result as disclosed on abstract and page 7, lines 2-6 where it is dynamically adapt to the security threats (selection based on the detection of the type of the virus as it has been detailed on col.3, lines 29-67 and col.4-6).

d) Applicant's admittance of the Prior Art (AAPA) disclose different detection methods of malicious code using heuristics logic as described on page 1 and 2 of the specification as Prior Art.

Therefore the motivation to combine such methods in Joyce are set forth in the limitation "AV systems using heuristic logic may use self-educating techniques to improve performance" as described by the Applicant on page 1 of the specification, and it is in harmony with Joyce's dynamic adaptation to the security threats on col.7, lines 2-6.

In conclusion Applicant's arguments traversing the examiner motivation to combine Joyce with AAPA are not persuasive.

2- As per applicant's arguments that Joyce does not disclose "repeating the analyzing and determining steps" which includes "determination of a probability of accuracy of a result of an additional analysis", examiner referes applicats to the following remarks:

a) Joyce disclose analyzing of the detected malicious codes and selection of the appropriate action based on the analyzed determination as disclosed on fig.4 and associated text; and col.1, lines 50-60. lines 54-57 of col.1 disclose such analyzing are done in accordance with "a level of confidence" regarding the harmfulness of the analyzed packets. therefore Joyce teach a probability of accuracy of the result of the analyzing where " a level of confidence" corresponds to applicant's probability of the accuracy. Further more line 57-59 of the col.1 also disclose assigning confidence rating and that corresponds to applicant's "predetermined level" of the claims language.

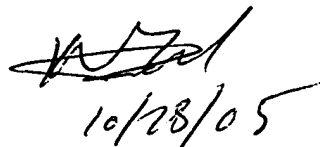
b) Joyce disclose selection of the packets for further analysis based on their assigned rating or determination level and that is the repeating the analysis of the detected malicious code as described on col.1, lines 57-59. Furthermore analyzing are based on the dynamic constant basis based on the monitoring of the packet streams (see abstract and summery of the invention). also see col.2 for detailed. therefore these are repeated process based on the detection of the malicious codes or viruses or attacks on the system. Applicant's arguments are not persuasive in that manner.

3- AS per Applicant's arguments that a user determines the determination level by inputting a value, examiner referes applicant's to the following remarks:

Examiner considers the firewall rule base 12 or 14 as corresponding to the Applicant's user whre the assigned rating on col.1, line 57-59 correponds to the Applicant's assigned or inputed value in order to construct a determined level or rating for analysis of the incoming packets.

In conclusion examiner would reconsider if the inputed value of the user be incorporated into the independent claims in the manner that distinguishes the applicant's invention from Joyce invention and AAPA, however such suggested amendment by the examiner should not raise new issues that necessiate further consideration or/and search, and have support in the specification.

4- Applicant has not responded to examiner requests (a and b) disclosed on the page 3 of the final action mailed on 08/01/2005 in order to facilitate the undrestanding of applicant's invention improvement over the prior art as the specification is mute in that regards.

  
10/28/05